Firmware Version: V2.40.046
Prom Code Version: V1.10.009
Published: 2015/06/01

These release notes include important information about D-Link DXS-3600 Series firmware revisions. Please verify that these release notes are correct for your switch:

- If you are installing a new switch, please check the hardware version on the device label; make sure that your switch meets the system requirement of this firmware version. Please refer to Revision History and System Requirement for detailed firmware and hardware matrix.

- If the switch is powered on, you can check the hardware version by typing "show system" command or by checking the device information page on the web graphic user interface.

- If you plan to upgrade to the new firmware release, please refer to the Upgrade Instructions:

D-Link switches support firmware upgrade via TFTP server. You can download the firmware from D-Link web site http://tsd.dlink.com.tw, and copy the downloaded firmware to the TFTP server folder. Please make sure that the TFTP server is accessible from the switch via networks.

For more detailed information regarding DXS-3600 Series switch products, please refer to Related Documentation.

You can also download the switch firmware, D-View modules and technical documentation from http://tsd.dlink.com.tw.

Content:

Revision History and System Requirement

Firmware Version	Date	Model	Hardware Version
Runtime: v2.40.046 PROM: v1.10.009	2015/6/1	DXS-3600-16S DXS-3600-32S	B1
Runtime: v2.00.023 PROM: v1.10.009	2013/9/30	DXS-3600-16S DXS-3600-32S	B1
Runtime: v1.10.023 PROM: v1.10.007	2012/8/31	DXS-3600-16S DXS-3600-32S	B1
Runtime: v1.00.024 PROM: v1.00.007	2011/12/26	DXS-3600-32S	A1

Firmware Version	Supported module		
Runtime: v1.10.023 and later Prom: v1.10.007 and later	DXS-3600-EM-8T DXS-3600-EM-4XT DXS-3600-EM-8XS	DXS-3600-EM-4QXS DXS-3600-PWR-FB DXS-3600-PWR-BF	DXS-3600-FAN-FB DXS-3600-FAN-BF
Runtime: v1.00.024 Prom: v1.00.007	DXS-3600-PWR-FB DXS-3600-FAN-BF	DXS-3600-FAN-FB	DXS-3600-PWR-BF

Upgrade Instructions:

Note1: User has to upgrade the software version to R2.31beta FIRST before upgrading the switch to R2.40.046. We recommend using the CLI instructions FIRST for firmware upgrade as the WEB UI will not support Boot Up Image selection until it is upgraded to R2.40.046 and later.

Note2: EI & SI features are all included in the firmware. While upgrading, system will automatically distinguish it and enable the associated features only.

Note3: v1.10.023 and later versions only work for B1 hardware version and NOT backward compatible to A1 hardware version. The v1.00.024 only works for A1

D-Link switches support firmware upgrade via TFTP server. You can download the firmware from D-Link web site http://tsd.dlink.com.tw, and copy the downloaded firmware to the TFTP server folder. Please make sure that the TFTP server is accessible from the switch via networks.

Upgrade using CLI (serial port)

Connect a workstation to the switch console port and run any terminal program that can emulate a VT-100 terminal. The switch serial port default settings are as follows:

- Baud rate: **115200**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**

The switch will prompt the user to enter his/her username and password. It should be noted that upon the initial connection, there is no username and password by default.

To upgrade the switch firmware, execute the following commands:

Command	Function
copy tftp://location/filename flash: filename	Download firmware file from the TFTP server to the switch.
boot image flash filename	Change the boot up image file.
show boot	Display the information of current boot image and configuration.
reboot	Reboot the switch.

Example:

DXS-3600-32S#copy tftp: //192.168.0.27/firmware.had flash: run.had

Address of remote host [192.168.0.27]
Source filename [firmware.had]
Destination filename [run.had]
Accessing tftp://192.168.0.27/ firmware.had...
Transmission start...
Transmission finished, file length 5156864 bytes.
Please wait, programming flash... Done

DXS-3600-32S#
DXS-3600-32S#configure terminal
**DXS-3600-32S(config)#**boot image firmware.had

DXS-3600-32S#sh boot

Unit 1
Boot image : /c:/2.40.046.had
Boot config : /c:/config.cfg

DXS-3600-32S#reboot
Are you sure you want to proceed with the system reboot? (y|n) y
Please wait, the switch is rebooting...

Upgrading by using Web-UI

1. Connect a workstation installed with java SE runtime environment to any front panel ports of the device and also connect console cable to switch's console port.

2. Enter switch's default IP address, 10.90.90.90 with subnet mask 255.0.0.0 into the address bar of the browser and press the Enter key.
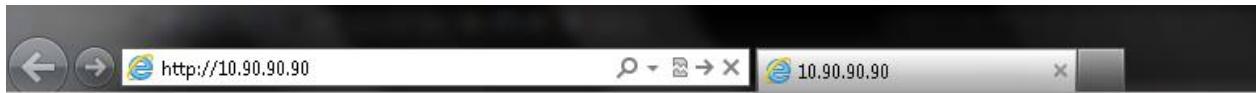
3. A user authentication window will be opened, by default, there is no user name and password configured on the switch. Just leave the **User Name** and **Password** fields blank and click the Login button.

4. Firmware upgrade from TFTP: click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP**

   Enter the TFTP Server's IP address and the source and destination file name in associated fields and then click **Upgrade** button.

5. Firmware upgrade from HTTP: click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**

   Select the switch's unit and then click **Browse** button to find the file name, specifying the destination file name. Click **Upgrade** to start the process.

6. Select the boot up image: click **Management > File System** to open the **File System** window

Click c: hyperlink, the following window will appear.

Click **Boot Up** button to set a specific runtime image as the boot up image.

7. Reboot the system: click **Tool > Reboot System**, as shown below; click **Reboot** to reboot the switch. When rebooting the switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings

New Features

Firmware Version	New Features

V2.40.046	1 All software features in R2.00.023 version can be supported by R2.40.046's Web GUI, MIB files and D-View module.
	
	2 The following new features are supported in CLI only
	   ● IS-IS routing protocol for both IPv4 and IPv6
	   ● IPv4 PIM Snooping
	   ● Multicast Source Discovery Protocol (MSDP)
	   ● PIM6-SSM
	   ● Per VLAN based IP Multicast Boundary on IPv4
	   ● G.8032v2 (ERPSv2)
	   ● VLAN Counter
	   ● IPv6 Stateless Address Autoconfiguration (SLAAC)
	   ● BFD (Bidirectional Forwarding Detection)
	   ● Selective Q-in-Q is able to work with MPLS
	   ● MPLS PHP is able to support implicit-null when running as LER/LSR
	   ● The management port is able to support AAA with TACACS+ and RADIUS server
	   ● Support RADIUS attribute 4, the NAS-IP-Address attribute
	   ● Scheduling Reboot
	   ● Be able to clear Telnet/ SSH session
	   ● IP DHCP Relay's destination supports specifying a Virtual Routing and Forwarding (VRF) space
	
	3 The following features' specification has been changed.
	   ● The LACP group number enlarges to 32 groups.
	   ● The DHCP Relay group number enlarges to 30 groups.

V2.00.023	1 Support Physical Stacking
	   ● DXS-3600-32S with DXS-3600-EM-Stack stacking module and DEM-CB50CXP, the 120G CXP Direct Attach Cable, can support 480G stacking bandwidth
	   ● DXS-3600-16S/32S with DXS-3600-EM-4QXS, the 40G expansion module and DEM-CB100QXS/300QXS, the 40G QSFP+ Direct Attach Cable, can support 160G stacking bandwidth
	
	2 Support Virtual Stacking
	
	3 The Layer 2 function supports following new features:
	   ● Loopback Detection (LBD)
	   ● L2 Protocol Tunneling
	   ● Ethernet Ring Protection Switching (ERPS)
	   ● Limited IP Multicast (IGMP Snooping Filter)

- Proxy Reporting
- MLD Snooping
- Multicast VLAN

4   The VLAN function supports following new features

- Private VLAN
- Super VLAN
- VLAN Translation

5   Support Explicit Congestion Notification (ECN)

6   The ACL function supports following new features

- ACL Statistics
- CPU Interface Filtering

7   The Security function supports following new features

- IPv6 SSH
- SSL v1/v2/v3
- IPv4/v6 SSL access
- D-Link Safeguard Engine
- BPDU Attack Protection
- ARP Spoofing Prevention
- DHCP Snooping
- DHCPv6 Guard
- Route Advertisement (RA) Guard
- IPv6 Snooping which contains following features
  - DHCPv6 Snooping
  - IPv6 ND Snooping
- IPv6 Source Guard
- IPv6 Neighbor Discovery (ND) Inspection
- DHCP Server Screening

8   The AAA function supports following new features

- Web-based Access Control (WAC)
- MAC-based Access Control (MAC)
- Microsoft® Network Access Protection (NAP)
- Compound Authentication
- Authentication Database Failover

9   The L3 function supports following new features

- Gratuitous ARP
- ARP Proxy
- Loopback Interface
- Null Interface
- RIPng
- OSPFv3

- RIPng and OSPFv3 are able to configure the Route Preference parameter
- Static Route supports IPv6 address
- Default Route supports IPv6 secondary route and Route Redistribution
- Route Redistribution supports IPv6 static route, RIPng and OSPFv3
- IPv6 Tunneling

10 The Green function supports following new features

- Green v1.0 supports power saving by link status and cable length
- Green v3.0 supports power saving by shutting down port or main chipsets
- Energy Efficient Ethernet (EEE)

11 The Management function supports following new features

- Web UI supports IPv6 address
- IPv6 Telnet Server and Telnet Client
- IPv6 TFTP and FTP client
- Secure FTP (SFTP) server
- Remote Copy Protocol (RCP)
- SNMP over IPv6
- Inconsistency airflow notification
- IPv6 log server
- Simple Mail Transfer Protocol (SMTP)
- RMONv1 & RMONv2 support getting information through SNMPv6
- sFlow
- IPv4 BootP client
- DHCP client supports DHCPv6 client and option 12
- DHCP Auto Configuration
- IPv6 Stateless Address Autoconfiguration (SLAAC)
- IPv6 DHCP Server
- DHCP Server supports option 60, 61, 82
- DHCPv6 Relay Agent
- Trusted Host
- IPv6 Path MTU Discovery
- IPv6 Ping and Traceroute
- Microsfot® Network Load Balancing (NLB)
- DNS Relay supports IPv6 and AAAA record
- IPv6 Neighbor Discovery Protocol
- When errors are detected in Management Port, switch is able to send traps or keep logs

12 The OAM function supports following new features

- Cable Diagnostic
- 802.3ah Ethernet Link OAM
- Connectivity Fault Management (CFM)

- Y.1731
- Optical Transceiver Digital Diagnostic Monitoring (DDM)

13   The L3 Multicasting function supports following new features
- IGMP Source Specific Mapping (SSM)
- IGMP/MLD Proxy
- IPv6 PIM-Sparse Mode (SM)
- PIM-Source Specific Multicast (PIM-SSM)
- Multicast Listener Discovery (MLD) v1/v2

14   Support IPv6 Core Ready logo phase II certification

15   Support IP-MAC-Port Binding which is composed by following functions:
- ARP Inspection
- IP Source Guard
- DHCP Snooping
- DHCPv6 Guard
- Route Advertisement (RA) Guard
- IPv6 Snooping
- IPv6 Source Guard
- IPv6 Neighbor Discovery (ND) Inspection

V1.10.023

1   Support DXS-3600-16S/32S B1 hardware version

2   Support Data Center Bridging (DCB) features which include
- 802.1Qaz Enhanced Transmission Selection (ETS)
- 802.1Qbb Priority-based Flow Control (PFC)
- 802.1Qau Congestion Notification (QCN)

3   Support below MPLS features
- MPLS Label-Forwarding
- MPLS QoS
- MPLS Ping & Trace Route
- LDP
- MPLS LSP Trigger Filter
- VPWS
- VPLS
- L2 Protocol Tunneling Through PW(pseudowire)
- Pseudowire redundancy

4   Support below L3 VPN features
- MPLS/BGP L3 VPN
- VRF-Lite
- MP-BGP

5   Support VRF Aware Application which includes
- Socket API

	• Telnet • DHCP Server/Relay • Ping • Trace route • FTP, TFTP • SNMP • Syslog • AAA • TACAS+ • RADIUS Servers
V1.00.024	First release, please refer to datasheet and manual for detail function support

Changes of MIB & D-View Module

The new features of MIB file are also included in the corresponding D-View module. Please download the D-View module on http://tsd.dlink.com.tw. For detailed changes of MIB content, please refer to the modification history in each MIB file.

Firmware Version	MIB File	New Features
V2.40.046	DLINKSW-DHCP6-SERVER-MIB	Modify SYNTAX to "DisplayString" for following object types: - dDhcp6SPoolAddrAssignClientDuid - dDhcp6SPoolPdClientDuid
	DLINKSW-ROUTE-MAP-MIB	Add new following new objects - setIpv6RecursiveNexthop - setIpv6Precedence
	DLINKSW-OSPFV2-MIB	Add new "isis(5)" value for object dOspfv2RedistProtocol
	DLINKSW-OSPFV3-MIB	Add new "isis(5)" value for object dOspfv3RedistProtocol
	DLINKSW-BGP-MIB	Add new "isis(11)" value for object dBgpRedistProtocol
	DLINKSW-IP-ROUTING-MIB	Add new "isis(8)" and "slaac(9)" value for object dIpRoutingRouteSummarySrcType
	DLINKSW-RIP-MIB	Add new "isis(5)" value for object dRipRedistProtocol
	DLINKSW-RIPNG-MIB	Add new "isis(5)" value for object dRipngRedistProtocol
	DLINKSW-QOS-MIB	Add ETS, the new QoS scheduling mode, in dQosSchedulingModeTable
V2.00.023	None	
V1.10.023	MPLS MIB	New MIB to support MPLS features
	L3 VPN MIB	New MIB to support L3 VPN features

	LLDP DCBX MIB	New MIB to support Data Center Bridging Exchange Protocol (DCBX)
	IP MIB	
	LED-DXS-3600-16S	
	General-mgmt	Add new table "swGenExpansionModuleMgmtTable" to General-mgmt MIB to support expansion modules
V1.00.024	First release, please refer to datasheet for detail MIB support	

Changes of Command Line Interface

The section below only shows command line changes that may bring backward compatibility issues with configuration settings for previous version of firmware.
Any new feature commands that do not have backward compatibility issues are not included in the below section.

Note: When upgrading the firmware from version R1.10 to R2.00; if configuration file is saved in the flash first and then processes the upgrade procedure, the switch will automatically convert the CLI commands to new format.

Firmware Version	Changes
V2.40.046	None
V2.00.023	1. AAA (Authentication, Authorization and Accounting) commands ● aaa changes to aaa new-model ● aaa authentication network default method1 [method2...] changes to aaa authentication dot1x default METHOD1 [METHOD2...] ● aaa authorization exec {default | list-name} method1 [method2...] is replaced by aaa authentication login {default | list-name} method1 [method2...] ● aaa authorization console is removed as when user passes the authentication, the console will accept the predefined authorization level which is configured in AAA server ● authorization exec {default | list-name} is replaced by authentication login {default | list-name} ● aaa local authentication attempts max-attempts is removed; the switch will accept 3 times attempt by default ● aaa local authentication lockout-time lockout-time is removed; the switch's lockout time is 60 seconds by default ● aaa authorization network default method1 [method2...]

is replaced by

aaa authentication [dot1x|mac-auth|jwac|web-auth] default method1 [method2 …]

- show aaa server group
  is replaced by
  show running-configure, for example *show running-config all | begin AAA*

- show aaa authentication {login | enable | network}
  is replaced by
  show running-configure, for example *show running-config all | begin AAA*

- show aaa authorization {exec | network}
  is removed as authentication and authorization functions are not separated, hosts will be authorized automatically after successfully authenticated

- show aaa accounting {exec | network}
  is replaced by
  show running-configure, for example *show running-config all | begin AAA*

- show aaa application [{line | http | network}]
  is replaced by
  show running-configure, for example *show running-config all | begin AAA*

- following commands
  - radius-server key text-string
  - tacacs-server key string
  - radius-server retransmit retries
  - radius-server timeout seconds
  - tacacs-server timeout seconds

  are replaced by
  radius-server host

- show radius-server configuration
  is replaced by
  show running-configure, for example *show running-config all | begin AAA*

- show tacacs-server configuration
  is replaced by
  show running-configure, for example *show running-config all | begin AAA*

2. Network Access Authentication commands

- network-access guest-vlan VLAN-ID
  changes to
  authentication guest-vlan VLAN-ID

- network-access authentication-mode {port-based | host-based}
  changes to
  authentication host-mode {multi-host | multi-auth [vlan VLAN-ID [,|-]] }

- dot1x timeout quiet-period <sec 0-65535>
  changes to
  authentication timer restart <SECONDS 1-65535>

- dot1x timeout reauth-period <sec 1-65535>
  changes to
  authentication timer reauthentication <SECONDS 1-65535>
- dot1x reauthentication
  changes to
  authentication periodic
- dot1x system-max-user <int 1-4096>
  changes to
  authentication max users <NUMBER 1-4096>
- dot1x port-max-user <int 1-4096>
  changes to
  authentication max users <NUMBER 1-4096>
- show network-access guest-vlan
  is replaced by
  show running-configure, for example

  Switch#show running-config all | begin COMP
  # COMPOUND_AUTHENTICATION

  configure terminal
   interface ethernet 2/0/1
     authentication guest-vlan 1
   end
- show network-access auth-configure [interface <interface-id>]
  is replaced by
  show running-configure, for example *show running-configue all | begin COMP*

3. DoS Prevention commands
   - defense [land | blat | null-scan | xmascan | tcp-synfin | port-less-1024 |
     ping-death | tiny-frag] enable
     changes to
     dos-prevention [all | land | blat | tcp-null-scan | tcp-xmas-scan | tcp-syn-fin | tcp-syn-srcport-less-1024 | ping-death | tcp-tiny-frag]
   - show defense
     changes to
     show dos-prevention [all | land | blat | tcp-null-scan | tcp-xmas-scan |
     tcp-syn-fin | tcp-syn-srcport-less-1024 | ping-death | tcp-tiny-frag]

4. Port Security commands
   - switchport port-security [{mac-address <mac-address> [vlan <vlan-id>]
     | mac-address sticky [<mac-address> [vlan <vlan-id>]]}]
     changes to
     switchport port-security [mac-address [permanent]<mac-address> [vlan
     VLAN-ID]]
   - clear port-security {all | configured | dynamic | sticky} [{address <mac-

dlink green

address> | interface <interface-id>}]
changes to
clear port-security {all | {address <mac-address> | interface [<interface-id> | <interface-list>]} [vlan VLAN-ID] }

5. DHCP Relay commands
   - ip dhcp relay information option82
     changes to
     ip dhcp relay information option

   - following commands are replaced by "class", "option hex" and "pool" parameters
     - ip dhcp relay option60
     - ip dhcp relay option60 identifier desc 255 relay ip-address [exact-match | partial-match]
     - ip dhcp relay option60 default relay ip-address
     - show ip dhcp relay option60 [identifier desc 255 | default]
     - ip dhcp relay option61
     - ip dhcp relay option61 identifier {string desc 255 | mac-address macaddr} {relay ip-address | drop}
     - ip dhcp relay option61 default relay ip-address
     - show ip dhcp relay option61

6. Traffic Segmentation commands
   - switchport protected unidirectional { tenGigabitEthernet PORTLIST | gigabitEthernet PORTLIST | fortygigabitethernet PORTLIST }
     changes to
     traffic-segmentation forward interface { range Ethernet PORTLIST | Ethernet PORT }

7. BPDU Protection commands
   - spanning-tree bpdu-protect { enable | disable }
     changes to
     spanning-tree bpdu-protection { drop | block | shutdown }

8. 802.1X commands
   - dot1x reauthentication
     changes to
     dot1x re-authentication

   - dot1x re-authenticate { interface <interface-id> | mac-address <mac-address> } in Global Configuration Mode
     changes to
     dot1x re-authenticate [interface INTERFACE-ID [mac-address MAC-ADDRESS]] in Privileged EXEC Mode

   - dot1x initialize { interface <interface-id> | mac-address <mac-address> } in Global Configuration Mode
     changes to
     dot1x initialize [interface INTERFACE-ID [mac-address MAC-ADDRESS]] in Privileged EXEC Mode

- dot1x system-max-user <int 1-4096>
  changes to
  authentication max users <NUMBER 1-4096>
- dot1x port-max-user <int 1-4096>
  is replaced by
  authentication max users <NUMBER 1-4096>
- remove dot1x system-fwd-pdu command, this version does not support configuring global system forwarding PDU capability, only supports per interface configuration, for example *(config-if)#dot1x forward-pdu*

9. SSH commands

- ip ssh port <int 1-65535 >
  changes to
  ip ssh service-port TCP-PORT

10. Storm Control commands

- storm-control {broadcast | multicast | unicast} {pps pps-rise [pps-low] | level level-rise [level-low]}
  changes to
  storm-control { {broadcast | multicast | unicast} level { pps PPS-RISE [PPS-LOW] | kbps KBPS-RISE [KBPS-LOW] | LEVEL-RISE [LEVEL-LOW] }}
- storm-control action { block | shutdown | drop }
  changes to
  storm-control action { shutdown | drop | none }

11. FDB commands

- clear mac-address-table filtering [address *MAC-ADDR* | vlan *VLAN-ID*] and clear mac-address-table static [address *MAC-ADDR* | interface *INTERFACE-ID* | vlan *VLAN-ID*] commands
  change to
  no mac-address-table static {all | *MAC-ADDR* vlan *VLAN-ID* [interface *INTERFACE-ID*] [, | -] }; the static parameter will include both original static and filtering parameters
- mac-address-table filtering *MAC-ADD* vlan *VLAN-ID*
  changes to
  mac-address-table static *MAC-ADDR* vlan *VLAN-ID* {interface *INTERFACE-ID* [, | -] | drop}
- no mac-address-table filtering *MAC-ADD* vlan *VLAN-ID*
  changes to
  no mac-address-table static {all | *MAC-ADDR* vlan *VLAN-ID* [interface *INTERFACE-ID*] [, | -] }
- mac-address-table notification [interval *SECONDS* | history-size *VALUE*]
  changes to
  mac-address-table notification change [interval *SECONDS* | history-size *VALUE*]
- snmp trap mac-notification {added | removed}
  changes to

snmp trap mac-notification change {added | removed}

- show mac-address-table notification [interface *INTERFACE-ID* | history]
  changes to
  show mac-address-table notification change [interface [*INTERFACE-ID*] | history]

- show mac-address-table count command
  is replaced by other show mac-address-table commands

  - show mac-address-table
  - show mac-address-table dynamic
  - show mac-address-table static

- show mac-address-table filtering [address *MAC-ADDR* | vlan *VLAN-ID*]
  changes to
  show mac-address-table [dynamic | static] [address *MAC-ADDR* |
  interface [*INTERFACE-ID*| vlan *vlan-id*], the filtering parameter is
  replaced by static

12. LLDP commands

- lldp message-tx-hold-multiplier value
  changes to
  lldp hold-multiplier VALUE

- lldp reinit-delay seconds
  changes to
  lldp reinit SECONDS

- lldp message-tx-interval seconds
  changes to
  lldp tx-interval SECONDS

- lldp-med fast-start-repeat-count value
  changes to
  lldp fast-count VALUE

- "lldp notification" and "lldp-med notification-topo-change"
  changes to
  lldp [med] notification enable"

- lldp-med tlv-select [inventory-management | capabilities]
  changes to
  lldp med-tlv-select [capabilities | inventory-management]

- lldp-dcbx tlv-select [ets-configuration | ets-recommendation | pfc-
  configuration]
  changes to
  lldp dot1-tlv-select dcbx [ets-configuration | ets-recommendation | pfc-
  configuration]

- lldp-dcbx run
  is removed as when LLDP is enabled, LLDP-DCBX will be enabled
  automatically in this version

- lldp notification-interval seconds

is removed; the notification interval will be 5 seconds by default.

- show lldp statistics
  changes to
  show lldp traffic
- show lldp statistics interface interface-id [, | -]
  changes to
  show lldp traffic interface INTERFACE-ID [, | -]
- show lldp local interface interface-id [, | -] {brief | normal | detail}
  changes to
  show lldp local interface INTERFACE-ID [, | -] [brief | detail]
- show lldp remote interface interface-id [, | -] {brief | normal | detail}
  changes to
  show lldp neighbors interface INTERFACE-ID [, | -] [brief | detail]
- The following original show commands for LLDP, LLDP-MED and LLDP-DCBX
  - show lldp-med
  - show lldp-med interface interface-id   [, | -]
  - show lldp-med local interface interface-id   [, | -]
  - show lldp-med remote interface interface-id   [, | -]
  - show lldp-dcbx interface INTERFACE-ID
  - show lldp-dcbx local interface INTERFACE-ID
  - show lldp-dcbx remote interface INTERFACE-ID

  are combined into following commands
  - show lldp
  - show lldp interface INTERFACE-ID
  - show lldp local interface INTERFACE-ID
  - show lldp neighbors interface INTERFACE-ID

13. Syslog commands
- logging buffered [LEVEL] | [write-delay { SECONDS | INFINITE }]
  changes to
  logging buffered [severity {severity-level | severity-NAME} | discriminator NAME][write-delay {SECONDS | infinite }]
- logging console [LEVEL]
  changes to
  logging console [severity {severity-level | severity-NAME}] [discriminator NAME]
- logging source interface INTERFACE-ID
  changes to
  logging source-interface INTERFACE-ID
- logging trap LEVEL
  is replaced by
  logging server

- logging facility FACILITY-TYPE
  is replaced by
  logging server
- logging on
  is replaced by
  logging buffered [severity {severity-level | severity-NAME}]
  [discriminator NAME][write-delay {SECONDS | infinite }]
- "logging count" and "show logging count" commands
  are replaced by
  show logging
- "save log" and "logging file flash"
  are removed as the log will be automatically saved when rebooting the
  switch

14. Debug commands

- error-reboot enable
  changes to
  debug reboot on-error
- clear error-log
  changes to
  debug clear error-log
- clear debug buffer
  changes to
  debug clear buffer
- Following commands

  - copy error-log tftp <IPADDR> <PATH_FILENAME >
  - copy debug buffer tftp <IPADDR> <PATH_FILENAME >
  - copy tech-support tftp <IPADDR> <PATH_FILENAME >

  change to

  - debug copy {buffer | error-log | tech-support} SOURCE-URL {tftp:
    //LOCATION/DESTINATION-URL
    |ftp: //USER-NAME:PASSWORD@LOCATION:TCP-PORT/
    DESTINATION-URL|rcp://USER-NAME@LOCATION/DESTINATION-
    URL } [vrf VRF-NAME]
- show error-log
  changes to
  debug show error-log
- show debug buffer [utilization]
  changes to
  debug show buffer [utilization]
- show tech-support
  changes to
  debug show tech-support
- show debug status

changes to

debug show output

- show error-reboot

  is replaced by

  show running-config | include debug

15. Device commands

- show cpu

  changes to

  show cpu utilization

- show memory

  changes to

  show unit

- logging-server enable device

  is replaced by

  logging discriminator

- show device-status

  is replaced by

  show environment [fan | power | temperature]

- show system-info

  is replaced by following commands

  - show unit

  - show version

  - show ip interface

16. RMON commands

- rmon event number [log] [trap community] [description description-string]

  changes to

  rmon event INDEX [log] [[trap COMMUNITY] [owner NAME] [description TEXT]

- show rmon event

  changes to

  show rmon events

17. SNMP commands

- no enable service snmp-agent

  is replaced by

  no snmp-server

- no snmp-server host {IP-ADDRESS [vrf NAME]}

  changes to

  no snmp-server host {IP-ADDRESS | IPV6-ADDRESS }

- snmp-server community   COMMUNITY-STRING view VIEW-NAME {ro | rw}

  changes to

  snmp-server community [0| 7] COMMUNITY-STRING [view VIEW-NAME]

[ro | rw] [IP-ACL-NAME]

18. CLI Basic commands

- show bootup-config

  changes to

  show startup-config

19. Configuration commands

- show bootup-config

  changes to

  show startup-config

- execute flash: *FILENAME*

  is replaced by

  copy flash: running-config

- boot config flash *FILENAME*

  changes to

  boot config *URL*

- copy running-config { bootup-config | flash: [*FILENAME*] | {   tftp:

  [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] } [vrf *VRFNAME*] }

  changes to

  copy running-config { startup-config | flash: [*FILENAME*] | {   tftp:

  [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] | rcp:

  [*//username@location/filename*] } [vrf *VRFNAME*] }

- copy bootup-config { running-config | flash: [*FILENAME*] | { tftp:

  [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] } [vrf *VRFNAME*] }

  changes to

  copy startup-config { running-config | flash: [*FILENAME*] | { tftp:

  [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] | rcp:

  [*//username@location/filename*] } [vrf *VRFNAME*] }

- copy { flash: [*FILENAME*] { bootup-config | running-config | { tftp:

  [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] } [vrf *VRFNAME*] }

  | { tftp: [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] } [vrf *VRFNAME*]

  { bootup-config | running-config | flash: [*FILENAME*] } }

  changes to

  copy { flash: [*FILENAME*] { startup-config | running-config | { tftp:

  [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] | rcp:

  [*//username@location/filename*] } [vrf *VRFNAME*] } | { tftp:

  [*//location/filename*] | ftp:

  [*//username:password@location:tcpport/filename*] | rcp:

[*//username@location/filename*] } [vrf *VRFNAME*] { startup-config | running-config | flash: [*FILENAME*] } }

- boot system flash *FILENAME*
  changes to
  boot image [check] *URL*

20. Password Recovery commands

- password-recovery
  changes to
  service password-recovery

- clear { levelpassword | username | configure }
  changes to following commands
  - password-recovery
  - no username
  - no enable password
  - no login console
  - show username
  - show running-config

21. LACP commands

- aggregateport load-balance {dst-mac | src-mac | src-dst-mac | dst-ip | src-ip | src-dst-ip }
  changes to
  port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac | dst-l4-port | src-dst-l4-port | src-l4-port }

- port-group *<value 1-16>* [static] and
  port-group mode {active | passive}
  change to
  channel-group *<value 1-16>* mode {on| active| passive}

- show aggregateport {[*<value 1-16>*] summary | load-balance} and
  show lacp summary
  change to
  show channel-group [channel [*<value 1-16>*] { detail | neighbor} | load-balance | sys-id]

22. Interface and IP commands

- interface out-band <int 1-1>
  changes to
  interface mgmt 0

- ip domain-lookup
  changes to
  ip domain lookup

- ip telnet server enable
  changes to
  ip telnet server

- arp timeout <min 0-65535> original command mode was Global

Configuration Mode and changes to Interface Configuration Mode in R2.0 software version

23. Mirror commands

- no monitor session *SESSION-NUMBER* destination interface *INTERFACE-ID* [acl *NAME*]
  is separated to following commands

  - no monitor session *SESSION-NUMBER* destination interface *INTERFACE-ID*

  - no monitor session *SESSION-NUMBER* source acl *ACCESS-LIST-NAME*

- no monitor session all
  is replaced by
  no monitor session SESSION-NUMBER

- show monitor [session *SESSION-NUMBER*]
  changes to
  show monitor session [*SESSION-NUMBER* | remote | local]

24. File System commands

- ls directory
  is replaced by
  dir

- cp dest {destine_file | directory} sour source_file and
  cp sour source_file dest {destine_file | directory}
  are replaced by
  copy

- rm filename and
  del filename
  are replaced by
  delete FILE-URL

- makefs dev devname fs fsname and
  makefs fs fsname dev devname
  are replaced by
  format FILE-SYSTEM [fat32 | fat16]

- pwd &
  cd directory
  are replaced by
  cd [DIRECTORY-URL]

25. ACL commands

- the following commands

  - ip access-list standard {[id|name]}

  - ip access-list extended {[id | name]}

  - mac access-list extended {[id | name]}

  - expert access-list extended {[id | name]}

  - ipv6 access-list *name*

  are changed to

- ip access-list [extended] NAME [*NUMBER*]
- mac access-list extended *NAME* [*NUMBER*]
- expert access-list extended *NAME* [*NUMBER*]
- ipv6 access-list [extended] *NAME* [*NUMBER*]

the *NAME* of ACL changes to necessary parameter not an optional one

- ip access-list resequence {id | name} start-sn inc-sn
  changes to
  access-list resequence { NAME | NUMBER } STARTING-SEQUENCE-NUMBER INCREMENT
- ipv6 traffic-filter name {in | out}
  changes to
  ipv6 access-group { NAME | NUMBER } [in|out]
- match ip address { acl_name | acl_id }+8
  changes to
  match ip address { ACL-NAME | ACL-NUMBER }
  R2.0 only supports one entry in VLAN sub map
- match mac address { acl_name | acl_id }+8
  changes to
  match mac address { ACL-NAME | ACL-NUMBER }
  R2.0 only supports one entry in VLAN sub map
- [sn] {permit | deny} {source-mac-address mask | host source-mac-address | any} {destination-mac-address mask | host destination-mac-address | any} [*ethernet-type*] [cos out [inner in]]
  changes to
  [SEQUENCE-NUMBER] { permit | deny } { any | host SRC-MAC-ADDR | SRC-MAC-ADDR SRC-MAC-WILDCARD} { any | host DST-MAC-ADDR | DST-MAC-ADDR DST-MAC-WILDCARD} [ethernet-type TYPE MASK] [cos VALUE [inner INNER-COS]] [vlan VLAN-ID   [inner INNER-VLAN]] [time-range PROFILE-NAME]
- [sn] {permit | deny} protocol [vlan out [inner in]] {source source-wildcard | host source | any} {source-mac-address mask | host source-mac-address | any} {destination destination-wildcard | host destination | any} {destination-mac-address mask | host destination-mac-address | any} [precedence precedence] [tos tos] [fragments] [time-range time-range-name]
  changes to
  [SEQUENCE-NUMBER]{permit|deny} PROTOCOL   { SRC-IP-ADDR SRC-IP-WILDCARD | host SRC-IP-ADDR | any} {SRC-MAC-ADDR SRC-MAC-WILDCARD | host SRC-MAC-ADDR | any} { DST-IP-ADDR DST-IP-WILDCARD | host DST-IP-ADDR | any} { DST-MAC-ADDR DST-MAC-WILDCARD | host DST-MAC-ADDR | any} [vlan OUTER-VLAN[inner INNER-VLAN]] [[precedence PRECEDENCE]   [tos TOS] |dscp DSCP] [time-range PROFILE-NAME]

In R2.0, the "protocol" parameter changes to optional
● the following commands
- [sn] {permit | deny} tcp [vlan out [inner in]] {source source-wildcard | host source | any} {source-mac-address mask | host source-mac-address | any} [operator port]] {destination destination-wildcard | host destination | any} {destination-mac-address mask | host destination-mac-address | any} [operator port] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [tcp-flag]
- [sn] {permit | deny} udp [vlan out [inner in]] {source source-wildcard | host source | any} {source-mac-address mask | host source-mac-address | any} [operator port] {destination destination-wildcard | host destination | any} {destination-mac-address mask | host destination-mac-address | any} [operator port] [precedence precedence] [tos tos] [fragments] [time-range time-range-name]
- [sn] {permit | deny} icmp [vlan out [inner in]] {source source-wildcard | host source | any} {source-mac-address mask | host source-mac-address | any} {destination destination-wildcard | host destination | any} {destination-mac-address mask | host destination-mac-address | any} [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]] [precedence precedence] [tos tos] [fragments] [time-range time-range-name]

are changed to
- [SEQUENCE-NUMBER] {permit|deny} tcp { SRC-IP-ADDR SRC-IP-WILDCARD | host SRC-IP-ADDR | any} {SRC-MAC-ADDR SRC-MAC-WILDCARD | host SRC-MAC-ADDR | any} [{eq | lt | gt | neq} PORT | range MIN-PORT MAX-PORT] { DST-IP-ADDR DST-IP-WILDCARD | host DST-IP-ADDR | any} { DST-MAC-ADDR DST-MAC-WILDCARD | host DST-MAC-ADDR | any} [{eq | lt | gt | neq} PORT | range MIN-PORT MAX-PORT] [vlan OUTER-VLAN[inner INNER-VLAN]] [[precedence PRECEDENCE] [tos TOS] | dscp DSCP [time-range PROFILE-NAME]
- [SEQUENCE-NUMBER] {permit|deny} udp { SRC-IP-ADDR SRC-IP-WILDCARD | host SRC-IP-ADDR | any} { SRC-MAC-ADDR SRC-MAC-WILDCARD | host SRC-MAC-ADDR | any} [{eq | lt | gt | neq} PORT | range MIN-PORT MAX-PORT] { DST-IP-ADDR DST-IP-WILDCARD | host DST-IP-ADDR | any} { DST-MAC-ADDR DST-MAC-WILDCARD | host DST-MAC-ADDR | any} [{eq | lt | gt | neq} PORT | range MIN-PORT MAX-PORT] [vlan OUTER-VLAN[inner INNER-VLAN]] [[precedence PRECEDENCE] [tos TOS] |dscp DSCP [time-range PROFILE-NAME]
- [SEQUENCE-NUMBER] {permit|deny} icmp{ SRC-IP-ADDR SRC-IP-WILDCARD | host SRC-IP-ADDR | any} {SRC-MAC-ADDR SRC-MAC-

WILDCARD | host SRC-MAC-ADDR | any} { DST-IP-ADDR DST-IP-
WILDCARD | host DST-IP-ADDR | any} { DST-MAC-ADDR DST-MAC-
WILDCARD | host DST-MAC-ADDR | any}   [ICMP-TYPE [ICMP-CODE]
| ICMP-MESSAGE] [vlan OUTER-VLAN[inner INNER-VLAN]]
[[precedence PRECEDENCE] [tos TOS] |dscp DSCP] [time-range
PROFILE-NAME]

The R2.0 version removes the support for configuring "fragment"
parameter for TCP/ UDP/ ICMP command. If users need to configure the
"fragment" parameter, they need to use "Protocol" ACL to accomplish it.

26. QoS commands
- match {access-group ACCESS-LIST-NAME | ACCESS-LIST-ID}
  changes to
  match {access-group name ACCESS-LIST-NAME}

R2.0 does not support ACL index and add a keyword name for this command.
If all configuration file are saved and then upgrade to R2.0, switch will
convert the command to new format automatically

- mls qos map dscp-cos DSCP-LIST to COS-VALUE in Global Configuration
  mode changes to Interface Configuration mode
- police sr-tcm BPS [bc BURST-NORMAL] [be BURST-MAX] conform-action
  ACTION exceed-action ACTION [violate-action ACTION] and
  police rate BPS BURST [exceed-action ACTION]
  change to
  police KBPS [BURST-NORMAL] [BURST-MAX] [conform-action ACTION]
  exceed-action ACTION [violate-action ACTION]
- police tr-tcm cir CIR [bc CONFORM-BURST] pir PIR [be PEAK-BURST]
  [conform-action ACTION [exceed-action ACTION [violate-action
  ACTION]]]
  changes to
  police cir CIR [bc CONFORM-BURST] pir PIR [be PEAK-BURST] [conform-
  action ACTION] [exceed-action ACTION [violate-action ACTION]]
- queue QUEUE-ID bandwidth MIN-BANDWIDTH-KBPS and MAX-
  BANDWIDTH-KBPS
  change to
  queue QUEUE-ID rate-limit MIN-BANDWIDTH-KBPS MAX-BANDWIDTH-
  KBPS
- hol_prevention is removed as this function will always be enabled in R2.0
- the following commands
  - show mls qos interface [INTERFACE-ID]
  - show mls qos rate-limit [interface INTERFACE-ID [,|-]]
  - show mls qos scheduler [interface INTERFACE-ID [,|-]]
  - show mls qos maps dscp-cos
  are combined to
  - show mls qos interface [INTERFACE-ID [,|-]] { cos | scheduler | trust

| rate-limit | queue-rate-limit | dscp-mutation | map {dscp-color | cos-color | dscp-cos} }

- the following commands
  - show mls qos interface [INTERFACE-ID] [policers]
  - show policy-map   [POLICY-NAME [CLASS-MAP-NAME]]

  are combined to
  - show policy-map [POLICY-NAME | interface INTERFACE-ID]

  R2.0 does not support CLASS-MAP-NAME optional parameter
- show interface [*INTERFACE-ID* [, | -]] priority-flow-control
  changes to
  show interfaces [*INTERFACE-ID* [, | -]] priority-flow-control
- qcn cnpv *CNPV-PRIORITY-VALUE*   [cp-creation { enable | disable }]
  changes to
  qcn cnpv *CNPV-PRIORITY-VALUE*   [cp-creation { auto-enable | auto-disable }]

27. OSPFv2 commands
- area <area_id>
  is removed as the area id can be created by other command
- route-preference ospf {intra-area <value> | inter-area <value> | external-1 <value> | external-2 <value>}
  changes to
  distance ospf { inter-area | intra-area | external-1 | external-2 } <value>
- ip ospf authentication [{message-digest | null}]
  changes to
  ip ospf authentication [message-digest]

28. BGP commands
- route-preference {ibgp|ebgp} value
  changes to
  distance bgp   EXTERNAL-DISTANCE INTERNAL-DISTANCE

29. VRRP commands
- vrrp vrid critical-ip ip-address
  changes to
  vrrp VRID track critical-ip IP-ADDRESS

30. RIP commands
- route-preference <value>
  changes to
  distance <DISTANCE>
- ip rip receive enable and
  ip rip send enable
  change to
  passive-interface {default | INTERFACR-ID}

31. Protocol Independent commands
- clear ip route and
  show ip ecmp load-balance

are changed to RD level commands
- the following commands
  - route-preference [vrf vrf-name] default value
  - route-preference [vrf vrf-name] static value

  are changed to
  - distance [vrf VRF-NAME] {static | default} DISTANCE
- ip ecmp load-balance [{sip | crc32_lower | crc32_upper} | dip | port](1)
  changes to
  ip route ecmp load-balance [{sip| crc32_lower| crc32_upper} | dip | port]
- show ip route-preference is replaced by show running-config
- show ip route [vrf vrf-name] [network [net-mask]] [{count | connected | static | rip | ospf | bgp | weight}]
  changes to
  show ip route [vrf VRF-NAME] [[ip-address [mask] | protocol] | hardware]
  show ip route summary [vrf VRF-NAME]

32. VLAN commands
- mac-base MAC-ADDRESS [priority COS-VALUE] in VLAN Configuration Mode
  changes to
  mac-vlan MAC-ADDRESS vlan VLAN-ID [priority COS-VALUE] in Global Configuration Mode

- subnet-base { NETWORK-PREFIX /PREFIX-LENGTH | IPV6- NETWORK-PREFIX /PREFIX-LENGTH } [priority COS-VALUE] in VLAN Configuration Mode
  changes to
  subnet-vlan { ipv4 NETWORK-PREFIX NETWORK-MASK | ipv6 IPV6-NETWORK-PREFIX / PREFIX-LENGTH } vlan VLAN-ID [priority COS-VALUE] in Global Configuration Mode
- switchport native vlan VLAN-ID
  changes to
  switchport hybrid native vlan VLAN-ID and
  switchport trunk native vlan { VLAN-ID | tag }

33. GVRP commands
- gvrp
  changes to
  gvrp global in Global Configuration Mode and
  gvrp enable in Interface Configuration Mode
- forbidden vlan VLAN-ID [,|-]
  changes to
  gvrp forbidden {all | VLAN-ID [, | -] | {add | remove} VLAN-ID [, | -] }

34. MPLS commands
- backoff maximum SECONDS

changes to

backoff INIT-TIME MAX-TIME

- mpls ldp hello-holdtime SECONDS and

 mpls ldp hello- interval SECONDS

 change to

 discovery hello { holdtime SECONDS | interval SECONDS }

- mpls ldp targeted-hello-accept

 changes to

 discovery targeted-hello accept

- targeted-hello { holdtime <seconds 15-65535> | interval <seconds 5-65535>}

 changes to

 discovery targeted-hello { holdtime SECONDS | interval SECONDS }

- ldp router-id IP-ADDRESS

 changes to

 router-id IP-ADDRESS

- transport-address {interface | IP-ADDRESS }

 changes to

 discovery transport-address {interface | IP-ADDRESS }

- mpls ldp distribution-mode {dod | du}

 changes to

 distribution-mode {dod | du}

- mpls ldp lsp-control-mode {independent | ordered}

 changes to

 lsp-control-mode {independent | ordered}

- mpls ldp max-path-vector VALUE

 changes to

 path-vector maxlength VALUE

- max-hop-count VALUE

 changes to

 maxhops VALUE

- mpls ldp targeted-peer IP-ADDRESS

 changes to

 neighbor IP-ADDRESS targeted

- mpls static l2vc-ftn VC-ID IP-ADDRESS out-label LABEL-VALUE

 changes to

 xconnect IP-ADDRESS VC-ID encapsulation mpls [manual] [raw| tagged] [mtu 0-65535]

- mpls static ilm in-label LABEL-VALUE forward-action pop-l2vc-destport INTERFACE-ID fec VC-ID IP-ADDRESS

 changes to

 mpls label LOCAL-LABEL REMOTE-LABEL

- class-map {inbound exp <VALUELIST 0-7> priority <VALUE 0-7> |

outbound [priority <VALUELIST 0-7>] exp < VALUE 0-7>}

changes to

following commands

- class map exp-cos EXP-LIST to COS-VALUE

- class map cos-exp COS-LIST to EXP-VALUE

- trust-exp

changes to

trust exp

- match {ip NETWORK-PREFIX/PREFIX-LENGTH }

changes to

match {ip NETWORK-PREFIX/PREFIX-LENGTH | vc IP-ADDRESS VC-ID }

- ping lsp NETWORK-PREFIX/PREFIX-LENGTH [times VALUE | timeout SECONDS]

changes to

ping mpls ipv4 NETWORK-PREFIX/PREFIX-LENGTH [repeat COUNT | timeout SECONDS]

- traceroute lsp NETWORK-PREFIX/PREFIX-LENGTH [timeout SECONDS]

changes to

traceroute mpls ipv4 NETWORK-PREFIX/PREFIX-LENGTH [timeout SECONDS]

35. Port commands

- interface {tenGigabitEthernet PORT | gigabitEthernet PORT | fortygigabitethernet PORT}

changes to

interface ethernet PORT

- interface range {tenGigabitEthernet PORTLIST | gigabitEthernet PORTLIST | fortygigabitethernet PORTLIST }

changes to

interface range ethernet PORTLIST

- medium-type {copper | fiber}

changes to

media-type {auto-select | rj45 | sfp}

- flowcontrol {auto | off | on}

changes to

flowcontrol {off | on}

- mtu

changes to

max-rcv-frame-size

36. Switch Controller commands

- enable asf

changes to

packet-forwarding asf

- show asf

is replaced by

show running-configure, for example *show running-config all | begin ASF*

37. VPWS commands

- xconnect *VC-ID IP-ADDRESS* encapsulation mpls [{raw | tagged}] [mtu 0-65535]

  changes to

  xconnect *IP-ADDRESS VC-ID* encapsulation mpls [manual] [raw| tagged] [mtu 0-65535]

- xconnect backup VC-ID IP-ADDRESS in "Interface Configuration Mode"

  changes to

  backup peer IP-ADDRESS VC-ID [delay {DISABLE-DELAY | never}] in "Xconnect Configuration Mode"

- encapsulation dot1q <vlanid 1-4094>

  changes to

  service encapsulation svid VLAN-ID

- The following commands

  - mpls static l2vc-ftn VC-ID IP-ADDRESS out-label LABEL-VALUE

  - mpls static ilm in-label LABEL-VALUE forward-action pop-l2vc-destport INTERFACE-ID fec VC-ID IP-ADDRESS

  changes to

  - mpls label *LOCAL-LABEL REMOTE-LABEL* in Xconnect Configuration Mode

38. VPLS commands

- vpls *VPLS-NAME*

  changes to

  l2 vfi *VPLS-NAME* manual

- vpls-id *VPLS-ID*

  changes to

  vpn id *VPN-ID*

- service-type {raw | tagged}

  changes to

  pw-type {raw | tagged}

- peer IP-ADDRESS [VC-ID] [{network | spoke}]

  changes to

  neighbor remote *IP-ADDRESS* [*VCID*] encapsulation mpls [no-split-horizon]

- peer backup *IP-ADDRESS* [*VC-ID*]

  changes to

  neighbor remote *IP-ADDRESS* [*VCID*] backup [delay {*DISABLE-DELAY | never*}]

- xconnect vpls *VPLS-NAME*

  changes to

  xconnect vfi *VPLS-NAME*

- clear mac-address-table vpls dynamic [*VPLS-NAME* [{peer *IP-ADDRESS* [*VC-ID*] | ac interface *INTERFACE-ID* [vlan *VLAN-ID*] | address *MAC-ADDR*}]]

  changes to

  clear mac-address-table vpls dynamic { all | *VPLS-NAME* [peer *IP-ADDRESS* [*VC-ID*] | ac *INTERFACE-ID* [vlan *VLAN-ID*] | address *MAC-ADDR*] }

39. Q-in-Q commands

- frame-tag tpid <hex 0x1-0xffff>

  changes to

  dot1q tunneling ethertype <hex 0x1-0xffff>

- show frame-tag tpid [interface *INTERFACE-ID*]

  changes to

  show dot1q ethertype [interface *INTERFACE-ID*]

- inner-priority-trust

  changes to

  dot1q-tunnel trust inner-priority

- insert-dot1q-tag <vlanid 1-4094>

  changes to

  dot1q-tunnel insert dot1q-tag <vlanid 1-4094>

- show switchport vlan mapping profile [interface *INTERFACE-ID*]

  is replaced by

  show dot1q-tunnel

40. MSTP commands

- the following commands

  - spanning-tree portfast [disabled]

  - spanning-tree autoedge [disabled]

  are combined into

  - spanning-tree portfast {disable | edge| network }

- spanning-tree tc-guard

  changes to

  spanning-tree tcnfilter

- spanning-tree external-cost COST

  changes to

  spanning-tree cost COST

- spanning-tree max-hops MAX-COUNT

  changes to

  spanning-tree mst max-hops HOP-COUNT

- spanning-tree hello-time SECONDS

  changes to

  spanning-tree mst hello-time SECONDS

- the following commands

  - show spanning-tree [summary | forward-time | hello-time | max-

age | tx-hold-count | max-hops]

- show spanning-tree interface INTERFACE-ID [{ portfast | link-type }]
- show spanning-tree mst { configuration | instance INTANCE-ID [interface INTERFACE-ID] }

change to

- show spanning-tree [interface [INTERFACE-ID [, | -]]
- show spanning-tree configuration interface [INTERFACE-ID [, | -]]
- show spanning-tree mst [configuration [digest]]
- show spanning-tree mst [instance INSTANCE-ID [, | -]] [interface INTERFACE-ID [, | -]] [detail]

41. IGMP Snooping commands

- ip igmp snooping mrouter {interface INTERFACE-ID [,|-] | forbidden interface INTERFACE-ID [,|-]}
  changes to
  ip igmp snooping static-group GROUP-ADDRESS interface INTERFACE-ID [,|-]

42. PIM commands

- ip pim old-register-checksum rp-address IP-ADDRESS
  changes to
  ip pim register-checksum-wholepkt rp-address-list ACCESS-LIST-NAME
- ip pim join-prune-interval SECONDS
  changes to
  ip pim jp-timer SECONDS

V1.10.023	None
V1.00.024	First release

Problem Fixed

Firmware Version	Problems
V2.40.046	1. Fix the backward compatible issue that if user configured IP interface with 10.x.x.x/8, the IP interface will be lost after upgrading the firmware. (DRU20130805000005, DRU20130918000004) 2. Fix the issue that user can access the switch via the console without authentication even if local authentication was enabled. (DRU20130415000001) 3. Fix the issue that DXS-3600 will filter DHCP Renew unicast packet when DHCP service was enabled. (DEUR20130415000008) 4. Fix the issue that the modification of port speed cannot be saved if user didn't configure the "duplex" parameter at the same time.

(DUSA20130530000004)

5. Fix the issue that the switch will change to exception mode due to improper coding for Path MTU time out timer configuration. (DRU20130613000002)

6. Fix the issue that user cannot disable HTTP and HTTPS at the same time. (DRU20131024000005)

7. Fix the issue that DXS-3600 did not forward OSPFv3 packet when OSPFv3 was enabled. (DI20131107000007)

8. Fix the issue that when user connected the expansion module DXS-3600-EM-4XT with DXS-3600, the ports on that expansion module will not link up in auto negotiation mode. (DRU20140131000004)

9. Fix the issue that the RX oversize statistics number was incorrect. (DRU20140226000003)

10. Fix the issue that when enabling IGMP Snooping in Q-in-Q, DXS-3600 will drop the IGMP packet whose packet size was less than 64 bytes. (DEUR20140331000011)

11. Fix the issue that the switch will not reply the IPv6 ping to a loopback interface. (DI20140408000004)

12. Fix the issue that when user configured IPv6 address on Loopback Interface and saved the configuration file. The IPv6 configuration will lost after rebooted the switch. (DI20140408000002)

13. Fix the issue that when user enabled ECMP on switch, the routing table may incorrect after running a period of time. (DI20140424000006)

14. Fix the issue that there was no response from many nodes when running Traceroute on the switch. (DRU20140421000006)

15. Fix the issue that in stacking architecture, the master switch did not synchronize the host key to slave switch when the SSH generating the RSA/DSA host key. (DI20140520000007)

16. Fix the issue that in stacking architecture, the member switches will change to pause mode when user turned off and then turned on the power of the master switch. (DI20140520000009)

17. Fix the issue that DXS-3600 will send duplicated TFTP control packets. (DI20140606000005)

18. Fix the issue that switch will not send or respond Neighbor Solicitation (NS) message after turning off the power of physical stacking's Master switch. (DI20140602000003)

19. Fix the issue that when user upgraded the firmware by TFTP, both the

Management and VLAN Interface will send TFTP request to TFTP server at the same time. (DI20140630000005, DI20120525000002, DI20121120000002)

20. Fix the issue that when user configured MLD Snooping with "filter-unregistered" parameter, DXS-3600 will not flood IPv6 Link-Local Multicast Name Resolution (LLMNR) or Simple Service Discovery Protocol (SSDP) packets. (DI20110914000006, DI20140411000006, DI20140630000004)

21. Fix the issue that the switch will not forward DHCP packets which were relayed by other switches. (DI20140708000005)

22. Fix the issue that the LSP sessions will be flapping after client being authenticated by TACACS+ server. (DRU20140815000004)

23. Fix the issue that the "class-map" configuration does not work correctly. (DRU20140814000001)

24. Fix the issue that when switch's port linked up and down, the L3 VPN service will fail to forward data. (DRU20141126000001)

25. Fix the issue that DXS-3600 will return an error message when user tried to enable the optical transceiver monitoring function with "transceiver-monitoring enable" CLI command. (DRU20141215000004)

26. Fix the issue that when user issued MPLS ping to Juniper switch, the ping will fail. (DRU20150203000005)

27. Fix the issue that when enabling LACP with Mirroring, the channel group load balancing algorithm did not work. (DRU20150225000003)

28. Fix the issue that the mirror configuration will loss after user upgraded the firmware. (DRU20150225000003)

29. Fix the issue that the system will prompt an error message when trying to delete an IP address. (DRU20150303000002)

30. Fix the issue that the switch might change to Pause mode when handling LSP packets. (DRU20150304000001)

V2.00.023

1. Fix the issue that when PC pings DXS-3600's IPv6 prefix address, not the switch's address, the switch still replies OK instead of ignoring it. (DUSA20130309000002)

2. Fix the issue that the configuration file cannot be transmitted completely via FTP server (DI20130108000006, DI20130313000001)

3. Fix the issue that when user enables VRRP and DHCP Relay on DXS-3600, if DHCP client sends a DHCP request to DHCP server, the server will receive duplicated DHCP request packets. (DI20130304000009,

	DI20130307000006, DI20130307000011, DI20130307000014, DI20130308000010, DI20130308000011)
	4. Fix the issue that when customer enables both Q-in-Q VLAN Translation and DHCP Relay service, DXS-3600 will not replace the VLAN ID. (HQ20130327000020)
	5. Fix the issue that when enables AAA local authentication for console port; user does not need to enter the user name and password when trying to access the switch via console port. (DRU20130415000001)
	6. Fix the issue that clients cannot get IP address when sending DHCP renew packet to DHCP server, the root cause is that DXS-3600 will filter the unicast DHCP renew packet when DHCP service is enabled. (DEUR20130415000008)
	7. Fix the issue that the modified port speed cannot be saved to configuration file if there's no "duplex" parameter followed the port speed modification command. (DUSA20130530000004)
V1.10.023	1. Fix the issue that when enabling Q-in-Q function, IGMP Snooping will not work.(DRU20120322000008)
	2. Fix the issue that when configuring TACACS key string via CLI, the key will be incorrect bug. (DRU20120329000002)
	3. Fix the issue that when executing command "show running-config", the display speed of pressing space bar for "next page" will be faster than the speed with "all" parameter in the command. (DEUR20120627000006)
	4. Fix the issue that when customer tries to connect to the switch via ssh protocol and needs to transmit lots of data by SSH server, such as executing "show log" or "show tech_support", the server will fail to transmit data to client and the client will also display "Incorrect MAC received on packet" error message. (DRU20120622000001)
V1.00.024	First release

* D-Link tracking number is enclosed in ()

Known Issues

Firmware Version	Issues	Workaround
V2.40.046	None	
V2.00.023	1. When executing "show environment" command, the display of "Detail Power Status" will show	It's a display bug and will not affect the

	"Internal Power" and "External Power" instead of "Power 1" and "Power 2".	whole function. This issue will be fixed in next release.
	2. Some of the CLI commands' format is different between R1.10 and R2.00. Users cannot execute the R1.10 original command in R2.00 version.	In order to prevent the previous configuration file missed after upgrading the firmware version to R2.00. Users can save the configuration files first before processing the upgrade.
	3. CVE-ID: CVE-2013-0149 Due to the ambiguous definition in OSPF protocol as specified in RFC2328, the attacker can send a false Link State Advertisement (LSA) which will evade the fight-back mechanism so that the LSA may be accepted and propagated by a "genuine" router on the network.	1. Enable MD5 authentication for OSPF 2. Enable OSPF Passive Interface to stop sending or receiving routing table update on interfaces that do not participate in OSPF 3. Enable MAC-based Access Control (MAC) to authenticate devices before they are able to communicate with the network
V1.10.023	None	
V1.00.024	None	

Related Documentation

- DXS-3600 Series Web UI Reference Guide Release 2.40
- DXS-3600 Series CLI Reference Guide Release 2.40
- DXS-3600 Series HW Installation Guide Release 2.40